ABOUT ME

• Ricky Magalhaes
• Over 20 years in cyber security
• A trusted advisor on several global boards
• Been in Data protection for over 15 years
Surveillance is the monitoring of behaviour, activities, or information for the purpose of influencing, managing or directing. This can include observation from a distance by means of electronic equipment.
**WHAT IS PRIVACY?**

*Privacy* is the ability of an individual or group to *seclude themselves*, or information about themselves, and thereby express themselves selectively.

The boundaries and content of what is considered private differ among cultures and individuals.
CHALLENGES OF SURVEILLANCE AND PRIVACY
WHO IS WATCHING?

These days, everyone

- Google
- Facebook
- Microsoft
- Instagram
- WhatsApp
- Amazon

But why?
Most data based companies like Google, Facebook, Social Media based companies are all funded by data mining and analytics.

The advertising is so targeted they can predict how we think and what we need.

We are addicted to being connected and these companies are all fighting for our attention and screen time.
IT’S A BUSINESS THEY MAKE MONEY

If its “free” YOU are the product!
IT’S A BUSINESS THEY MAKE MONEY

If it’s “free” YOU are the product!
PRIVACY IS OUR RIGHT

• Privacy has never been more under threat. But strangely, it has also never been more alive.
• From increasingly connected and personalized spaces to the looming threat of ubiquitous facial recognition, we are faced with unprecedented threats from governments and companies, who can [know more about us](#) than was ever previously possible.
WHO ELSE SPY'S ON US

- Malware
- Spyware
- Worms
- Foreign governments
- Crooks
- Telecommunication companies
- PIs
WHAT ABOUT AI?

• In the world of analytics even the bots will gather information about us
• Bio signature dynamics
• Keyboard strokes
• The way we hold our phones
• Our applications and data content
• Eventually the algorithms will be able to predict with 99% accuracy
ENCRYPT YOUR DATA WHERE YOU CAN

- It's simple to encrypt your data
- Use a VPN
- Turn off location tracking on your phone
- Disable GPS services if you don't need them
- Use secure Wi-Fi and or private connections
CAN I PROTECT MY PRIVACY?

1. Yes you can, Read the terms and conditions
2. make sure you are happy to trade privacy for services
3. Disable tracking and take the time to turn it off
4. Companies like apple are aware of this and in the next version of the OS will make it simpler
5. The industry is adapting to make it easier
6. We all need to challenge service providers to register with the commission
7. The SPs need to follow the rules if they don’t do not use them if you can
WHAT ABOUT THE CLOUD

• Is it safe?
• Can others (service providers) read my stuff?
• How do we thwart surveillance?
Thank you for your attention,

I hope you found this valuable

Ricky Magalhaes 2020
Who we work with!
<table>
<thead>
<tr>
<th>Concerns</th>
<th>Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Not knowing what data you process!</td>
<td>• Data Activity Register</td>
</tr>
<tr>
<td>• No clear policies and procedures in place!</td>
<td>• Data Protection Policy</td>
</tr>
<tr>
<td>• No processor agreements in place!</td>
<td>• List of all processors</td>
</tr>
<tr>
<td>• Don’t know if I need to comply with Jersey, UK or the GDPR laws!</td>
<td>• Territorial scope assessment</td>
</tr>
</tbody>
</table>
- Know what data you process
- Look for vulnerabilities / exposure on a regular basis
- Train your staff
- Have easily accessible policies and procedures
- Know your processors and who has access to your data
- Train your staff
• Leave data lying around for people to see, read or photograph
• Give access to your data to a 3rd party without an agreement in place
• Think it will go away
• Not train your staff
Discussion Points

- REGISTRATION WITH THE OIC
- AGREEMENTS
- GDPR – ADDITIONAL POSSIBLE REQUIREMENTS
- TRAINING
- CCTV
- IMPACT ASSESSMENTS
The Breach of 2019
Coping with immediate impact, how it felt & lessons learnt
Welcome to the LibertyBus shop

You can use this site to add pay as you go credit to your AvanchiCard, renew your AvanchiCard travel passes, manage your account and more - letting you beat the queues and never need change for the bus again.

To get started, you’ll need to register your AvanchiCard and create an account - after that topping up or renewing online couldn’t be easier.
How we found out
What we did

Password Updated!

Your password has been changed successfully.
Use your new password to log in.
Communications

Dear Customer

We are contacting you because we have learned of a reported data security incident on the LibertyBus website. We can confirm that your personal information has not been compromised, but as a valued customer we understand that you may be worried.

A thorough investigation has been conducted and we can confirm that the information stolen was limited to email addresses, AvanchiCard numbers, and passwords. Those who have been directly affected by this phishing scam have already been contacted.

Please be aware that LibertyBus will never ask for personal financial information via email. If you have any questions or concerns, please contact us at info@libertybus.com.
What support we had
Customer reaction
What we learnt

Honesty is the best policy
DATA PROTECTION WEEK

#ItsAllAboutYou

27 - 31 January 2020
10 Essential Data Protection Questions Every Board Should Ask

Advocate Caroline Dutot
“Good governance never depends on laws but on the personal qualities of those who govern...”

Frank Herbert, American Author
1. Is there a data audit/data map/data privacy impact assessment?
2. What personal data is held?
3. Where is personal data held?
4. How is personal data used?
5. How long is personal data kept for?
6. How secure is the personal data?
7. Who is the personal data shared with? Is it yours to share?
8. What would be the impact of a data breach to your business – worst case scenarios/biggest challenges?
9. What technical and organisational measures are in place to manage data risk?
10. What is your data breach scenario plan?
<table>
<thead>
<tr>
<th>How data received/Why obtained</th>
<th>Data type</th>
<th>Personal or special category data</th>
<th>Basis for processing</th>
<th>Controller/Processor</th>
<th>Where data held</th>
<th>Retention period</th>
<th>Security controls</th>
<th>Shared with who (additional details if shared outside EEA)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Website Enquiry</td>
<td>Name</td>
<td>Personal data</td>
<td>Legitimate interest</td>
<td>Controller</td>
<td>On database/spreadsheet</td>
<td>X period of time in order to reply to query</td>
<td>Pen testing of website</td>
<td>Not shared, unless have consent of the client/customer</td>
</tr>
<tr>
<td></td>
<td>Email</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>If they become a client/customer, retained for X period</td>
<td>Security controls around database have been confirmed by provider to apply security standard XYZ</td>
<td></td>
</tr>
</tbody>
</table>
AS A BOARD MEMBER YOU SHOULD EXPECT TO SEE AND APPROVE:

1. Data audit
2. Data protection policy
   (internal, employee directed)
3. Privacy notice
   (external, explanation to customers)
4. Opt in consent clauses
5. Controller & Processor agreements
Privacy notice

I. Who you are and what you do
II. What information of theirs you hold and why
III. How you obtained the information
IV. How you use the information
V. How long you retain the information
Privacy notice

VI. Whether you share the information, why and who with

VII. How they can request a copy of their data, have it deleted or rectified

VIII. Whether the data will be sent outside the EEA and safeguards in place

IX. Contact details for DPO (if required)

X. Right to Complain to JOIC
Example consent clause

Here at [organisation x] we value your privacy and we will only use your personal information to administer your account and provide products and services to you. However, from time to time we would like to contact you with details of:
(a) Other services we provide; (b) Updates; or 
(c) Competitions.
Please tick against each box that you would wish to receive information for....
GDPR quick compliance checklist

Have you:

→ Completed your data audit;

→ Updated or created: privacy notices, consent notices (including marketing consents and mailing lists) and data protection policies;

→ Reviewed contracts or terms and conditions with third parties;

→ Trained employees in GDPR and introduced any new changes in policies and procedures to employees;

→ Put in place a DPO, if needed; and

→ Given thought to the security measures that you have in place around personal data and whether further security measures are needed.
Infographic top 10 breaches
Summarised from breaches published by ICO, UK

**TOP 10 ERRORS**

1. Data compromised by cyber-attack
2. Documents kept in unlocked locations
3. Documents transported in an insecure manner
4. Unsolicited marketing approaches
5. Failing to respond to a subject access request
6. Failing to get adequate consent to use data
7. Sending personal data to your own email account without authorisation
8. Failing to ensure personal data on your network is properly secured
9. Failing to have effective security measures in place to protect data
10. Accessing records without a business need to do so (public authority)
Questions?
Advocate Caroline Dutot

Ardent Chambers

cdutot@ardentchambers.com
01534 481809
ABOUT ME

• Ricky Magalhaes
• Over 20 years in cyber security
• A trusted advisor on several global boards
• Been in Data protection for over 15 years
MANAGING SECURE DATA TRANSFERS

In this session we will cover:
Reduce Risk, Reduce cost, Manage Data

• The secure ways to transfer data
• What constitutes a breach
• What it takes to make data safe in transit and at rest
• Threats to avoid and how to minimise risk
WHERE IS DATA TRANSFERRED?

- On your network from your computer to your file server or repository
- This might be on premise or in the cloud
- We transfer data every day via email and web searches and downloads and uploads
- IoT/OT devices uploading and downloading data on our behalf
WHO IS INTERESTED IN OUR DATA?

• Everyone! Data is the new currency!
• Google
• Microsoft
• Amazon
• Facebook
• Service providers
IS MODERN SECURITY GOOD?

• People and being honest we are still complacent 5/10
• Most technical controls are documented but many not implemented 4/10
• TCs challenging to implement, picking the right one is hard 3/10
• The challenge is not dully understood as our data is everywhere 3/10
• The most basic controls like backups are not restorable 6/10
• What about TLS/HTTPS and certificates? That’s a very small part of the control not even 5%

Recent Global breach where the most basic control backup would have helped, RH
MY RRM MODEL
WHO ELSE SPY’S WANTS OUR DATA?

- Malware
- Spyware
- Worms
- Foreign governments
- Crooks
- Telecommunication companies
- PIs
WHAT IS MAN IN THE MIDDLE?

Avoiding **Man-in-the-Middle** Attacks
WHY ARE THEY INTERESTED IN YOUR DATA?

• To productise you, yes you are a product!
• To sell to you and your company
• To predict things
• To understand your habits and improve predictability which is not at 98-99%
SO WHAT CAN WE DO TO SECURE THE DATA TRANSFER?

• Use **strong access control** on the access to the data

• Be careful of who provides the service (MITM) Man in the Middle

• Read what you agree to and challenge the service provider on through this can we effect change

• **Encrypt** all data that you value, that you store and that you transfer

• If the encryption is provided by the service provider (BEWARE) as this is probably a trick

• **Monitor, Audit** the data at rest and data in transit, this will prove the integrity

• Ensure the data is highly **available** to the authorised users and the company
HOW DO MOST BREACHES OCCUR?

What are the primary causes of breaches?

Common reasons include:

- 46% A lost or stolen computing device
- 42% Employee mistakes or unintentional actions
- 42% Third party snafus
- 33% Criminal attack
- 31% Technical systems glitch
- 14% Malicious insider
- 8% Intentional non-malicious employee action

These breaches were discovered by:

- 52% audit/assessment
- 47% employee detected
- 36% patient complaint
IT’S A BUSINESS THEY MAKE MONEY

If its “free” YOU are the product!
IT’S A BUSINESS THEY MAKE MONEY

If its “free” YOU are the product!
• Privacy has never been more under threat. But strangely, it has also never been more alive.

• From increasingly connected and personalized spaces to the looming threat of ubiquitous facial recognition, we are faced with unprecedented threats from governments and companies, who can know more about us than was ever previously possible.
WHAT ABOUT THE CLOUD

• Is it safe?
• Can others (service providers read my stuff?)
• How do we thwart interception?
SOME MORE TIPS

• It's simple to encrypt your data
• Use a VPN
• Turn off location tracking on your phone
• Disable GPS services if you don’t need them
• Use secure Wi-Fi and or private connections
• Keep data in your control as much as possible
• Don’t send data out to the cloud without protection
• Monitor access to your systems and your data
CAN I PROTECT MY DATA SUMMARY?

1. Yes you can, Read the terms and conditions
2. make sure you are happy to trade privacy for services
3. Disable tracking and take the time to turn it off
4. Companies like apple are aware of this and in the next version of the OS will make it simpler
5. The industry is adapting to make it easier
6. We all need to challenge service providers to register with the commission
7. The SPs need to follow the rules if they don’t do not use them if you can
8. If you suffer a breach report it ASAP
THANKYOU

for your attention,

I hope you found this **valuable**

Ricky Magalhaes 2020
CCTV and Data Protection Impact Assessments

PropelFwd

Paul Byrne PC.dp (GDPR)
Managing Director
Who we work with!
How many organisations in this room use CCTV
### How many CCTV users have conducted a Risk Assessment

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Very Likely</th>
<th>Likely</th>
<th>Unlikely</th>
<th>Highly Unlikely</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fatality</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>Medium</td>
</tr>
<tr>
<td>Major Injuries</td>
<td>High</td>
<td>High</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>Minor Injuries</td>
<td>High</td>
<td>Medium</td>
<td>Medium</td>
<td>Low</td>
</tr>
<tr>
<td>Negligible Injuries</td>
<td>Medium</td>
<td>Medium</td>
<td>Low</td>
<td>Low</td>
</tr>
</tbody>
</table>
What are the main areas to consider?

- Why you want CCTV and is there an alternative solution?
- Where you are placing the cameras?
- What is your legal basis for using CCTV?
- What are the Risks?
- Who do I need to inform?

Consideration

Solutions

- Document your reasons and other considerations
- Know what you are allowed and what you are not allowed to do
- You have to have a legal basis for processing personal data
- Conduct a full DPIA
• Use signage to inform visitors to your premises that you use CCTV
• Have a clear CCTV policy in place and know how long to keep the images for
• Complete a DPIA, especially if you are recording a public area
• Remember the recorded image is somebody's personal data, protect it, secure it, delete it if not needed
• Have a clear procedure for disclosure
• Train your staff
• Let anybody view the images who are not authorised
• Give access to your data to a 3rd party without an agreement in place
• Keep the images ‘Just in case’ they are needed
• Forget CCTV images can form part of a subject access request
How do you do a DPIA?
DATA PROTECTION WEEK
#ItsAllAboutYou

27 - 31 January 2020

JOIC
JERSEY OFFICE OF THE INFORMATION COMMISSIONER
PRIVACY BY DESIGN

DATA PROTECTION WEEK 2020

DATE: 29TH JANUARY 2020
WORKSHOP AGENDA

• Define objectives
• What is Privacy by Design?
• The Privacy by Design framework
• Scenarios
• Tools & Technology
WHAT IS PRIVACY BY DESIGN?
WHAT THE LAW SAYS
Data Protection (Jersey) Law 2018

Part 2 - Fundamental Duties of Data Controllers
Article 6 - General duties and accountability

1) A controller -

(d) in planning and implementing the processing of personal data, must ensure that appropriate safeguards for the rights of data subjects are put in place by design and by default in accordance with Article 15;
Article 15 - Data protection by design and by default

(1) A controller must, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures that are designed to -

(a) implement the data protection principles in an effective manner; and

(b) integrate the necessary safeguards into the processing to meet the requirements of this Law and protect the rights of data subjects.
(2) In determining whether or not a measure is appropriate for the purposes of this Article, regard must be had to the state of technological development, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing.
WHAT THE LAW SAYS
Data Protection (Jersey) Law 2018

(3) The technical and organizational measures must ensure as far as practicable that, by default -

(a) only personal data that are necessary for each specific purpose of the processing are processed; and

(b) personal data are not made accessible to an indefinite number of natural persons without the data subject’s consent or other lawful authority.

(4) Paragraph (3) applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility.
WHAT THE LAW SAYS
EU GDPR 2016/679

Recital 78

In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default.
WHAT THE LAW SAYS
EU GDPR 2016/679

Article 25 - Data protection by design and by default

Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures
THE PRIVACY BY DESIGN FRAMEWORK
BACKGROUND

• Initially developed in 1995 by Information and Privacy Commissioner of Ontario, Dutch Data Protection Authority and Netherlands Organisation for Applied Scientific Research

• Adopted by International Conference of Data Protection and Privacy Commissioners (ICDPPC) in 2010

N.B. As of November 2019 ICDPPC is the Global Privacy Assembly
1. **Proactive not Reactive**
   The best way to mitigate a risk is to not introduce it in the first place

2. **Privacy as Default**
   Gives users confidence that their data is secure without explicit action on their part

3. **Embedded into Design**
   Consider privacy from the earliest stages of a project
THE 7 FOUNDATIONAL PRINCIPLES

4. Full Functionality
   There shouldn’t be a trade-off between privacy, security and functionality

5. End-to-End Security
   Data protection should be embedded throughout the data lifecycle

6. Visibility and Transparency
   Both for clients and for internal processes
THE 7 FOUNDATIONAL PRINCIPLES

7. Respect for User Privacy
   Put the user’s interests first. Make it user-centric.
**BENEFITS**

**Legal requirement** - best approach is to over-achieve so compliance is not in doubt.

**Differentiator** - seen as positive by clients, especially in light of recent ‘scandals’.

**Mitigate business risk** - protect your organisation. And you!

**Ethical/Moral** - putting individuals’ rights and freedoms first is a positive demonstration of corporate ethics
BARRIERS

Time - slow down delivery by adding additional requirements

Cost - need for extra resource

Priority - often not a concern for many organisations, especially if they haven’t suffered a breach

No associated income - for the most part this is about income retention not generation
SCENARIO 1 - NEW CRM SYSTEM

1. Your organisation is implementing a new CRM (Customer Relationship Management) system.

2. Your current client records are spread across some aging paper files and 2 spreadsheets. One for clients which have joined over the last 2 years and one for sales leads/opportunities.

3. Your RMs (Relationship Managers) also keep client information in their email accounts, with each RM adhering to their own filing system.

4. You have identified a couple of SaaS (software as a service) solutions as likely candidates based on some basic functional requirements and input from your RMs.

How do you ensure this project adheres to the Privacy by Design principles?
SCENARIO 2 - IMPLEMENTING CCTV

1. You work for a small conference centre that hires out rooms to businesses.
2. Two evenings a week, you rent a room to a local scout group.
3. Your organisation is implementing a basic CCTV system.
4. The cameras will be:
   a) in the shared foyer of the office building facing your main door
   b) inside the conference centre directed at the fire exit, which is in the staff kitchen

How do you ensure this project adheres to the Privacy by Design principles?
SCENARIO 3 - M&A

1. Your organisation is fitness gym providing workout facilities and group classes.
2. It has just bought a nutritional consultancy in order to increase the range of services it offers.
3. You have been tasked with integrating the newly acquired service lines into your organisation’s existing service offering and maximising the cross-selling potential.

How do you ensure this project adheres to the Privacy by Design principles?
DATA PROTECTION IMPACT ASSESSMENTS

The Law

Article 16 of Jersey DP Law

1) Where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons, a controller must carry out an assessment of the impact of the envisaged processing operations on the protection of personal data before the processing...

6) A data protection impact assessment must contain the following minimum requirements -

a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

c) an assessment of the risks to the rights and freedoms of natural persons referred to in paragraph (1); and

d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Law, taking into account the rights and legitimate interests of any person.
DATA PROTECTION IMPACT ASSESSMENTS

DPIAs

A DPIA is designed to help you systematically analyse, identify and minimise the data risks of a data processing activity. It can help you demonstrate compliance and assist you to document, manage and mitigate any risks.

In line with ‘privacy by design’ this process must be carried out before you commence the data processing activity. In this way, it is proactive and demonstrates that you have built in data protection from the outset, not as an afterthought.

A DPIA is a living document. Processing may change over time and new risks may emerge, so it will require periodic review.
DATA PROTECTION IMPACT ASSESSMENTS
High Risk

Is special category or criminal offence data being processed?
Is the data being processed used for profiling people?
Is data matched or combined from different sources?
Does the processing involve the profiling or targeting of children?
Is there sensitive nature data present?
Is this systematically monitoring the public on a large scale?
Does this processing use a ‘new technology’?
Does the processing track individuals’ location or behaviour?
Is there data about vulnerable individuals involved?
DATA PROTECTION IMPACT ASSESSMENTS

DPIAs

BEST PRACTICE

Even if there is no indication of likely high risk, it is good practice to conduct a DPIA for all new or changed processing.
DOCUMENTATION

- DPIAs
- Risks - owners, mitigating actions
- Data Processing Activities
- Data Assets - items, locations
- Service Providers - locations, contracts, data assets
DOCUMENTATION
Tools for Managing documentation
TECHNOLOGY
The Challenges

• Whilst technology can help it is also, potentially, the greatest source of risk

• Use of unsanctioned applications, known as “shadow-IT”. Users often co-opt “personal” tech for work, e.g. WhatsApp

• Two ways to stop “shadow-IT”:
  • carrot - ensure users have the functionality they need so that they don’t look elsewhere
  • stick - implement a solution to prevent users from accessing unsanctioned apps
TECHNOLOGY
Approaches

Least privilege
Only give access on a “need to know” basis -> proactive
Benefit - minimise data access, protecting client, company and staff.
Challenge - managing access -> push it to the business

Retention
Label data and use those labels to apply retention policies
Benefit - no need for reactive housekeeping tasks
Challenge - defining a simple labelling scheme and making the labelling process easy
TECHNOLOGY
Approaches

Encryption
Consistent use of an ‘industrial strength’ encryption tool
Benefit - significant mitigating factor in the event of a breach
Challenge - providing clear advice to staff on what/when to encrypt, impact on recipients

Default Behaviour
Collect minimal data and avoid providing default values
Benefit - reduced risk, improved data quality, increased adherence to privacy principles
Challenge - putting individual data privacy ahead of potential/perceived business benefit
Accountability encapsulates everything the GDPR is about...It formalises the move of our profession away from box ticking or even records of processing, and instead seeing data protection as something that is part of the cultural and business fabric of an organisation. And it reflects that people increasingly demand to be shown how their data is being used, and how it’s being looked after. But I’ll be honest, I don’t see that change in practice yet.

A public statement issued in April 2019 by Elizabeth Denham, UK ICO
THANK YOU

Phil Ruelle               Mel Pardoe
Chief Digital Officer    Group Data Protection Officer
BDO                      BDO
pruelle@bdo.je            mpardoe@bdo.je
SME – Data Protection workshop and solutions

PropelFwd


Paul Byrne PC.dp (GDPR)
Managing Director
Who we work with!
What type of business is in the room?
<table>
<thead>
<tr>
<th>Consideration</th>
<th>Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Do I have to register with the JOIC?</td>
<td>• If you collect personal data, then yes – register online</td>
</tr>
<tr>
<td>• What data do I collect?</td>
<td>• Have a good idea what data you collect, what type and what legal basis</td>
</tr>
<tr>
<td>• Do I really have to comply with the law?</td>
<td>• Anyone who processes data as a controller or processor, must comply with the law</td>
</tr>
<tr>
<td>• What measures do I have in place to protect peoples data?</td>
<td></td>
</tr>
<tr>
<td>• Do I have a website?</td>
<td></td>
</tr>
<tr>
<td>• How can I show compliance?</td>
<td></td>
</tr>
</tbody>
</table>
Do you have a Website?

Consideration

• Is it an information or commercial website?
• Do you have a privacy notice available to visitors?
• Do you use ‘Cookies’ on your site?
• Have you considered who else has access to any data you collect?
• Do you need a processor agreement?
How can I become compliant with the law?

Scalability & Proportionality

- Remember every organisation is different, so have different needs for compliance?
- Depending on the size of your business, you might only need a Privacy Notice or a small framework policy?
- Organisational and Technical measures need to be proportionate
- Have a clear plan in place?
- If you have staff, train them?
• Know what data you collect and process.
• Have a policy suitable for your business.
• Know who else you share data with.
• Secure the data you collect
• Have a clear procedure for disclosure
• Train your staff
• Let anybody view the data you collect who are not authorised.
• Give access to your data to a 3rd party without an agreement in place.
• Keep the data ‘Just in case’ it is needed.
• Ignore the requirements of the law just because you are an SME.
Data Protection Compliance

Process Improvement Training

Data Protection Officer / Adviser

Data Protection Training

Process improvement projects

EU Data Protection Representative

Data Protection Compliance

PropelFwd

Data Protection: Risks, Rights & Solutions

Aonghus Fraser
30th January 2020
Aonghus (Gus) Fraser

- Revoke CEO – www.revoke.com
- Technologist (Cybersecurity, Blockchain background)
- Data Protection & Privacy Advocate
- af@revoke.com
- Twitter: @gusfraser
Risks

So what? Why me?
Data misuse and breaches are out of control!

- 4.1 Billion accounts breached in 1st half of 2019!
- Marriott 500 Million accounts
- Lenovo 36TB
- BA 380,000 accounts
- Facebook 50 Million accounts
- Cambridge Analytica 87 Million accounts
- Equifax 146 Million accounts
Users have no idea how many companies have their personal data

- Even “ethical” companies like John Lewis share data with over 20 companies
- Hundreds of Data Warehouses and Tracking Companies trade personal data
- These companies have data breaches too; Apollo 126M accounts (July 2018)

Source: Financial Times
https://www.ft.com/content/9d741ea6-e73f-11e7-8b99-0191e45377ec
Facebook Must Face Lawsuit Over 29 Million-User Data Breach

By Kartikay Mehrotra and Aoife White
June 24, 2019, 9:44 AM GMT+1

NASA Data Breach Demonstrates Need for Proper Network Governance

A recent startup breach exposed billions of data points
Grindr shares personal data with ad companies in violation of GDPR, complaint alleges

A Norwegian nonprofit has filed three complaints against the company

By Jon Porter | @JonPorty | Jan 14, 2020, 12:25pm EST
Leaked Documents Expose the Secretive Market for Your Web Browsing Data

An Avast antivirus subsidiary sells 'Every search. Every click. Every buy. On every site.' Its clients have included Home Depot, Google, Microsoft, Pepsi, and McKinsey.
Ring doorbell 'gives Facebook and Google user data'
Off-Facebook activities

This is a summary of the 589 apps and websites that have shared your activity.

Some of your activity may not appear here. [Learn more]

SoundCloud Pulse: for Creators
Received 29 January 2020

gov.je
Received 23 January 2020

19 interactions were received.

How did Facebook get this activity?
This activity was shared using Facebook’s business tools.

What does Facebook do with your activity?
We use your activity to:
- Show you things that you might be interested in, such as events that you might want to go to.
- Show you relevant ads that introduce you to new products and services.
- We don’t reveal your information to gov.je.
- We don’t sell your information to anyone.

What you can do
- View gov.je
- Turn off future activity from gov.je
- Give feedback about this activity
So What?
If left in the wrong hands…
Your personal data can be used to:

• Steal your identity
• Scam You, your friends and family
• Steal your money
• Send you unsolicited marketing
• Blackmail you
• Leak private information
• Hijack your social media
• Make unauthorised purchases
• Damage your credit rating
• Take out loans in your name
<table>
<thead>
<tr>
<th>Event Description</th>
<th>Author/Manager</th>
<th>Date/Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Changed the country restrictions to only show the Page to people in Vietnam</td>
<td>Ads Manager V1.2659</td>
<td>8 Jan 2020, 21:23</td>
</tr>
<tr>
<td>Added Gus Fraser as an admin</td>
<td>Ads Manager V1.2659</td>
<td>8 Jan 2020, 20:39</td>
</tr>
<tr>
<td>Changed the name of Amber Long to Amber.</td>
<td>8 Jan 2020, 17:29</td>
<td></td>
</tr>
<tr>
<td>Removed Amber Long (Business Manager) from managing the Page</td>
<td>Amber Long</td>
<td>8 Jan 2020, 16:56</td>
</tr>
<tr>
<td>Claimed ownership of the Page</td>
<td>Ads Manager V1.2659</td>
<td>8 Jan 2020, 16:56</td>
</tr>
</tbody>
</table>
Rights

What are your legal rights as a consumer?
Request Data

• Request a copy of all personal data can be requested

• You might be surprised that companies hold on you!
Delete Data

• Request your data is deleted!
• Ever used a Price Comparison website?
• Ever switched telcos?
• Ever requested they delete your data..?
Solutions
Protect yourself, your family, your organisation
Alternatives & Awareness

• Watch “The Great Hack”
  • [www.thegreathack.com](http://www.thegreathack.com)

• Brave Browser
  • [www.brave.com](http://www.brave.com)

• DuckDuckGo Search Engine
  • [www.duckduckgo.com](http://www.duckduckgo.com)

• Ad blockers
Facebook

• Download your data
  • It may not be all.. do it anyway!
• Clean up apps & websites
• Delete “off-facebook” activity
• Do NOT answer “what kind of dog are you” or other quizzes..!
• Don’t accept random friend requests…
Location & App Permissions

• Be aware...
• Do they REALLY need this data? ALL the time…?
• Camera?
• Microphone?
Password Hygiene

• Password Manager (1Password, Dashlane, KeePass, LastPass)
• Strong master password (Phrase)
• Multi-factor Authentication
Password Best Practices (Cont.)

• Absolute minimum of 8 chars
• Check https://haveibeenpwned.com/Passwords
• Don’t re-use passwords
• Check https://howsecureismypassword.net/
Public WiFi

• Don’t!
• If you must... ensure you’re using a trusted VPN
• Read the Privacy Policy!
• Turn off AirDrop / File Sharing
Multi-Factor Authentication
Software Updates

• Windows Update & Patching
• Antivirus
• Most infamous breaches could have been prevented!
  • E.g. EternalBlue / WannaCry
Phishing, Clickbait & Malware

• Remain vigilant
• Check spelling
• Check language (salutation, signature)
• Don’t open unexpected attachments
Reduce your Digital Footprint

• Digital Self-Defence!
• Read Terms & Conditions & Policies!
• Close unused accounts; delete apps
• Exercise your Data Protection rights – right to Erasure!
• Risks assessment: don’t give away personal data when it shouldn’t be required
• Don’t complete click-bait surveys or quizzes
Revoke

- www.revoke.com
- Free in Jersey!
- Public launch March
- Early access February
Any Questions?
Thank You

Aonghus Fraser  
CEO  
af@revoke.com  
+44 7797 766 111  
www.revoke.com
ARTIFICIAL INTELLIGENCE
WHAT IS IT? DO ETHICS MATTER?

Data Protection Week
January 30, 2020, 1:00 pm – Digital Jersey Hub, St. Helier, Jersey

Gailina Liew BSc LLB MBA
“Can machines think?”

“Artificial Intelligence” term coined
Progress since 1950’s

- Following instructions
- Learning & improving through experience (without explicit programming)
- Moving beyond human experience

Artificial Intelligence

Machine Learning

Deep Learning
(neural networks) +
Many more algorithm types
Artificial Intelligence

- **REASONING** (solving problems with deductive logic)
  - Legal & financial asset management, autonomous weapons systems, games

- **KNOWLEDGE** (defining properties and classifying into categories)
  - Medical diagnosis, fraud prevention, purchase prediction, financial trading

- **PERCEPTION** (using sensory inputs)
  - Surveillance, self-driving vehicles, medical diagnosis

- **COMMUNICATION** (understanding written & spoken language)
  - Customer support, real-time written and spoken language translation, voice control

- **PLANNING** (setting sequence to achieve goal)
  - Scheduling, navigation, inventory management, predictive maintenance, logistics
Artificial Narrow Intelligence

Artificial General Intelligence

Artificial Super Intelligence

1997

2016

2017 – AlphaGo Zero
First robot citizen (Saudi Arabia)

Robotic and remote surgery

Sexbot

Carer

Assistant

AI enabling E-Justice, E-insurance, E-Discovery, Academic Assessment, Fraud Detection/Prevention, etc. ad infinitum...
AI – Looking Ahead

• AI market is projected to become a USD 190 Billion industry by 2025 (Markets and Markets)
• Chatbots will power 85% of customer service by 2020 (Innovation Enterprise)
• Chatbots are expected to cut business costs by USD 8 Billion by 2022 (Impactbnd)
• 63% of customers prefer messaging with online bot to communicate with business or brand (Mindshare)
• 46% of Americans use digital voice assistants (Pew Research Center)
• 30% of companies in the world will be using AI in at least one of their sales processes by 2020 (Venture Harbour)
• Share of jobs requiring AI skills has grown 4.5 times since 2013 (Forbes)
• AI will eliminate 1.8 million jobs and create 2.3 million by 2020 (Venture Harbour)
Mr Alcine tweeted Google about the fact its app had misclassified his photo
Bias In = Bias Out
Trustworthy AI and Ethical Use

April 2018  EU Guidelines for Ethical Use

May 2018  OECD published recommendations on AI
GDPR – Articles 21 & 22
Convention 108 of the Council of Europe – adopted by EU & UK

July 2018  UK published guidelines for use of AI in public sector

May 2019  OECD Principles on AI adopted by 42 countries
EU Guidelines – 7 Requirements

Includes detailed questions for companies/AI developers to address for each requirement. For example, regarding Societal & Environmental Wellbeing:

- Did you assess whether the AI system encourages humans to develop attachment and empathy towards the system?
- Did you ensure that the AI system clearly signals that its social interaction is simulated and that it has no capacities of “understanding” and “feeling”?
- Did you ensure that the social impacts of the AI system are well understood? For example, did you assess whether there is a risk of job loss or de-skilling of the workforce? What steps have been taken to counteract such risks?

Pilot testing with companies in progress with final set of questions targeted for publication in early 2020
Trust

We take the following definition from the literature: “Trust is viewed as: (1) a set of specific beliefs dealing with benevolence, competence, integrity, and predictability (trusting beliefs); (2) the willingness of one party to depend on another in a risky situation (trusting intention); or (3) the combination of these elements.”

While “Trust” is usually not a property ascribed to machines, this document aims to stress the importance of being able to trust not only in the fact that AI systems are legally compliant, ethically adherent and robust, but also that such trust can be ascribed to all people and processes involved in the AI system’s life cycle.

Trustworthy AI

Trustworthy AI has three components: (1) it should be lawful, ensuring compliance with all applicable laws and regulations (2) it should be ethical, demonstrating respect for, and ensure adherence to, ethical principles and values and (3) it should be robust, both from a technical and social perspective, since, even with good intentions, AI systems can cause unintentional harm. Trustworthy AI concerns not only the trustworthiness of the AI system itself but also comprises the trustworthiness of all processes and actors that are part of the system’s life cycle.
“Kasparov’s Law”

weak human + machine + better process
is superior to
strong human + machine + inferior process

“There’s nothing artificial about AI. It’s inspired by people, it’s created by people, and—most importantly—it impacts people. It is a powerful tool we are only just beginning to understand, and that is a profound responsibility.”

Fei Fei Li
THANK YOU!

gailina.liew@gmail.com

Gailina Liew BSc LLB MBA
NED - Jersey Data Protection Authority, Digital Jersey;
Executive Director - Jersey Policy Forum
Working from Home & Data Protection
Data Protection (Jersey) Law 2018

Our function:

• To make individuals aware of their rights

• To ensure public authorities and companies are aware of their responsibilities

• To conduct investigations into complaints by individuals about public agencies or companies concerning the management of personal data

• To manage the process of registration of public authorities and companies

• To investigate complaints that individuals bring to our attention
Principles of Good Personal Data Handling

- Lawfulness, fairness, transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity & confidentiality (security)
- Accountability
Data Privacy Impact Assessment (DPIA)

• Assess...
  • Special category data on living individuals (*health, political views, sexual orientation etc*).
  
  • Risk to data privacy is if a file is lost or mislaid.
  
  • If working for an organisation you may wish to consider...
    • Whether only parts of the file could be taken home to reduce the risk.
      
    • Whether there are other ways of working that would reduce or remove the risk of data loss in transit or at home.
      
    • Whether staff are properly trained on how to transport and use personal data when removing it from the office.
Security ‘Considerations’

• Permissions to take work home
• Records are kept of what is removed (& returned)
• Can only copies be removed?
• How the paperwork to be transported for example:  
  – in a locked briefcase  
  – not left in open view in a car
• How home working should be set up:  
  – Physical space where family members and visitors cannot see the paperwork  
  – Locked away securely when not in use
• How to report a lost file
Who needs to know you are working from home?

• If you are part of an organisation your manager needs to know in order to make assessment & ensure work is being done in accordance with data security and home working policies

• Consider having a sign-in / sign-out procedure for when taking files & personal data home

• Contracts of employment should have compliant data privacy clauses & refer to appropriate security, homeworking, transporting data rules

• Make sure everyone is aware of what to do if a file is lost & test the plan
What are the risks of a data breach when working from home?

• Being distracted whilst working at home and leaving your unlocked devices or loose paperwork unattended is easy to do...

• Remember, if an unauthorised person can access the computer or paperwork, this would classify as a data breach
Top tips!

• Have a private, secure place to work
• Do not leave unlocked devices unattended or paper work lying about
• Ensure secure WIFI and anti-virus software
• If you take work between the office and home, only take home what is absolutely necessary
• Ensure all paper files are secure in a locked device which is not accessible to anyone else
• Ensure staff are aware of how to report and handle a data breach if one should occur
• Ensure ‘working form home’ policies / contracts are in place and all staff are provided with adequate training
DATA PROTECTION WEEK

#It'sAllAboutYou

27 - 31 January 2020

JOIC JERSEY OFFICE OF THE INFORMATION COMMISSIONER